Halasz 2000-0249

REMARKS

Claims 1-51 were rejected under 35 USC 102 as being anticipated by Schuba et al, US Patent No. 6,725,378. Applicants respectfully traverse.

In support of rejecting claims 1, 13, 20, 23-24, and 31, the Examiner cites col. 3, line 46 through col. 4, line17, and col. 11 lines 39-49. The first-cited passage teaches the three-way handshake comprising a host sending a SYN packet to a destination, the destination sending a SYN+ACK packet to the source, and the source sending an ACK packet to the destinations. The packets are characterized by the flags that are set in the packets. The second-cited passage states that

> the frequency of unacceptable and/or band source SYN packets [is measured] using a conventional statistical model to predict arrival of the next spoofed SYN packet. A RST may be sent for any packets arriving in the spoofed time interval to enhance protection of the destination hosts 54. In still another embodiment suited to SYN flooding based on pseudorandom number generated addresses, routines may be implemented that detect use of pseudorandom sequences generated by various conventional generators to identify spoofed packets.

Comparing the teachings of the cited passages to, for example, claim 1, it is clear that only the above-quoted passage from col. 11 relates to the limitation of

> determining whether the first request and the second request have arrived at the host device within a predetermined time interval, the predetermined time interval being based on a probability distribution function of the arrival times of previous requests for starting data connections received at the host device from a given originating location;

What this executes is a *determination relative to a single packet* (i.e., the "second packet"). It answers the question: "Has a second packet arrived within X second of the first packet?" where X was selected based on past information. In contradistinction, the col. 11 passage teaches that from past information one can say something about the arrival rate of spoofed SYN packets; for example, one is able to make the statement: "On the average, there is one spoofed packet every 1.34 seconds." This passage does not deal with any one packet but, rather, deals with rates, and the solution proposed from this knowledge is to send an RST packets at the same identified rate. It should be appreciated that in consequence of the difference between the step specified in claim 1 and the teachings of the Schuba et al reference, the mode of operation is completely different. In

the method defined in claim 1 an action is taken relative to a received packet that was determined to have arrived before the expiration of the X second interval (i.e., too soon), such as refusing to accept it, or sending an RST packet (to match the action suggested by the reference). In other words, the determination is made that the packet is a packet intended to flood the target and action is taken relative to the packet. In the Schuba et al reference, in contradistinction, RST packets are sent at some average rate, placing reliance for preventing SYN flooding on averages. Both methods work, but the two methods are different and the two methods have different dynamic attributes. Accordingly, it is respectfully submitted that the claim 1 method is not anticipated by the Schuba et al reference, and neither are claims 2-12, which depend on claim 1.

Additionally, claim 1 defines an the action of denying the second data connection to the client. In Schuba et al, there is a an RST packet that is sent, but there is no correlation to such an RST packet and the denying of service to the very specific "second data connection. This is another reason for holding that claim 1 and the claims that depend thereon are not anticipated by Schuba et al.

Independent method claims 13 and 20 each specifies a step that, vis-à-vis the Schuba et al reference, has the same attributes as the step of determining in claim 1 and, therefore, it is respectfully submitted that claims 13 and 20 are not obvious in view of the Schuba et al reference, and neither are claims 14-19, which depend on claim 13, and claims 21-22, which depend on claim 20.

Independent claim 23 defines a system that includes a processing device and a program that executes a step of evaluating, claim 24 defines a computer-readable medium that includes a program that performs a step of evaluating, and claim 31 defines a means for determining. Vis-à-vis the Schuba et al reference, each of these limitation has the same attributes as the step of determining in claim 1 and, therefore, it is respectfully submitted that claim 23, 24, and 31 are not obvious in view of the Schuba et al reference, and neither are claims 25-30 which depend on claim 24, and claims 32-39 which depend on claim 31.

In support of rejecting claims 40 and 44 20, 23-24, and 31, the Examiner cites col. 3, line 34 through col. 4, line17. Applicants respectfully traverse. It is noted with some surprise that the Examiner has not cited the passage at col. 11 even though claim 40

has a step of determining that is not unlike the step found in claim 1 and which was discussed above, but regardless of the fact that the Examiner failed to cite that passage, the passage exists and, no applicants' remarks above apply. Moreover, the last clause of claim 40 specifies a step of signaling a network control center. No such step is taught by Schube at al, and certainly not in the passage cited by the Examiner. Therefore, claim 40 is not anticipated by Schuba et al, and neither are claims 41-43 which depend on claim 40.

Independent claim 44 defines a step of determining and a step of signaling a network control center that, vis-à-vis the Schuba et al reference, correspond to the claim 40 limitations discussed above. It is respectfully submitted, therefore, that claim 44 is not anticipated by Schuba et al, and neither are claims 45-51 which depend on claim 44.

For sake of brevity, the above remarks do not address the various limitations of the dependent claims that also make the claims allowable, but it should be understood that in fact many of the claims do have such distinguishing limitations, contrary to the Examiner's assertions. To give just one example, claim 5 specifies calculating a difference value in the arrival times of the first request and the second request. In rejecting the claim the Examiner cited col. 5, lines 14-57. However the cited passage does not teach anything about measuring time difference between the arrival times of two connection requests. The only reference to time in that passage is that a timer is set to (usually) 75 seconds between the SYN and SYN-RECVD messages of a particular single connection request. Aside from the fact that that is a wholly different notion, measuring time in any event is not the same as measuring whether a certain time is smaller than a preselected threshold value. In short, in applicants' view passage cited by the Examiner does not come even close to that which claim 5 specifies.

Halasz 2000-0249

In light of the above, it is respectfully submitted that all of the Examiner's rejections have been overcome. Reconsideration and allowance of the subject claims are, therefore, solicited.

Respectfully,
Sylvia Halasz
Kamlesh T. Tewani

Dated: 8/22/05

By _____
Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net